**PHIT presentation:** **October 22, 2003**

**Dept of Health**
**Technology Overview**
**Connectivity with our Trading Partners**

**Drivers – "Raising the Bar"** (Privacy and Security)
- ☑ Federal-level (HIPAA, Bio-Terrorism, Homeland Security, Gramm-Leach-Bliley, Sarbanes-Oxley, others)
- ☑ State-level (Executive orders, WACs, RCWs, statewide IT security policies, SB 1386 - CA)
- ☑ Move to the Internet for access by external trading partners (Digital Government)
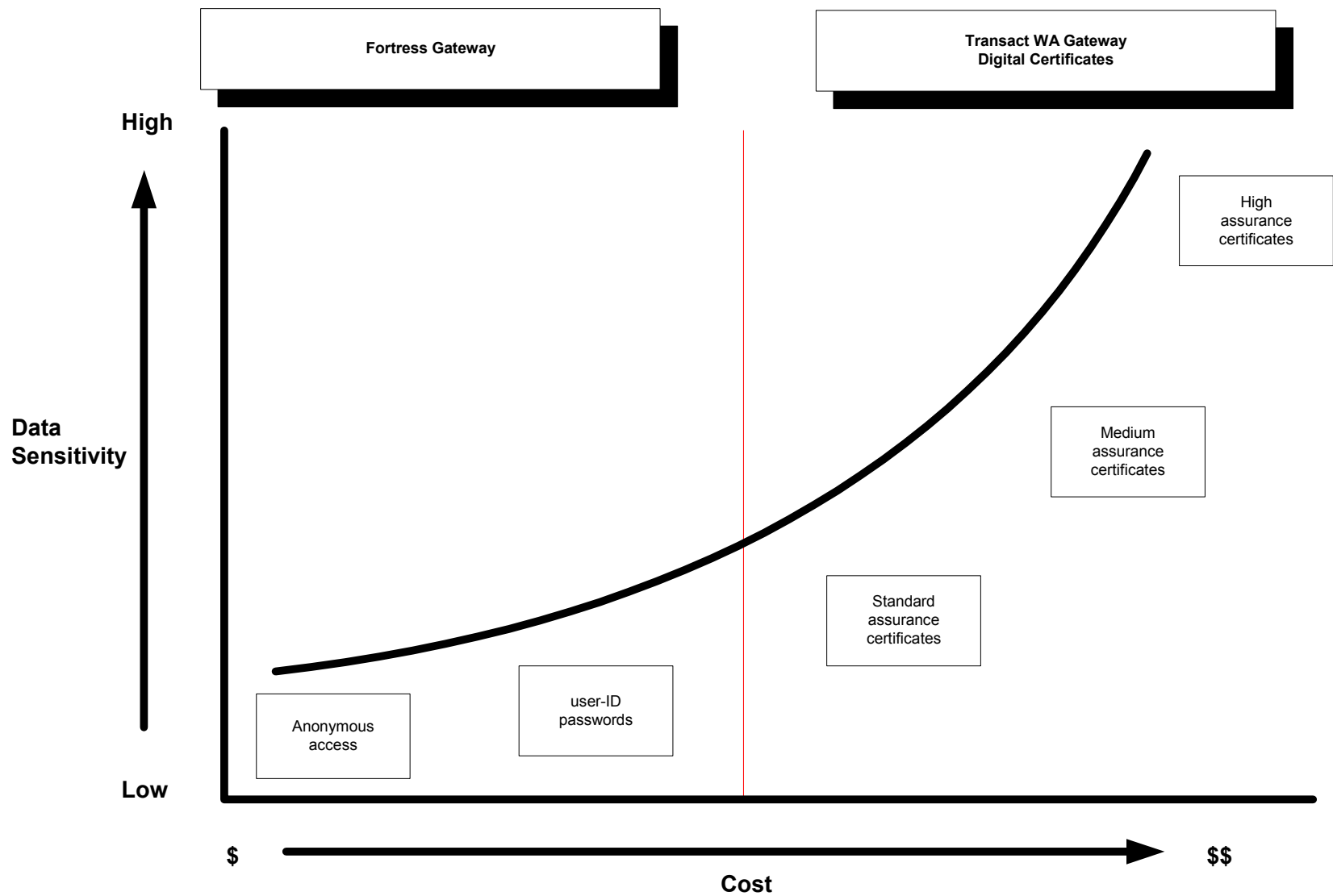- ☑ Confidential nature of health industry data

**Architecture strategies**
- ☑ Secured environments for Internet-based applications
- ☑ Authentication gateways (portals)
- ☑ Secured data file transfers
- ☑ Continuum of security technologies to meet varying security requirements

**Trading partner requirements**
- ☑ Near current Operating Systems (NT 4 – Win 2000 – XP)
- ☑ Security technologies
  - o Web browser (SSL/TLS compatible, 128 bit encryption)
  - o Secure file transfer (SFT) software (web browser, SFT client, VPN client)
  - o Secure communications (Alerts – Content management – Public Health directory)
  - o Digital certificates (authentication, electronic signatures, encryption)

State of Washington
Authentication Gateways

Fortress Gateway

Transact WA Gateway
Digital Certificates

High

Data Sensitivity

Low

High assurance certificates

Medium assurance certificates

Standard assurance certificates

user-ID passwords

Anonymous access

$ — Cost — $$

Application Architecture (logical)
WA State secured web systems

IGN

State Agencies

Internet

Authentication Gateway

State Secure Network

AGENCY NETWORK

**Protected Environment**

1. Secured site
2. Encrypted sessions
3. Proxied access
4. Authenticated access
5. Segregated functions

Web Application Server

DMZ